

#2
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Takeo OHISHI

Serial No. 09/836,325

Filed: April 18, 2001

For: AUTHENTICATION SYSTEM, AND
CONTENTS-INFORMATION
SENDER AND RECEIVER



Art Unit: 2131

Examiner:

Atty Docket: 0102/0162

SUBMISSION OF PRIORITY DOCUMENTS RECEIVED

Assistant Commissioner for Patents
Washington, D.C. 20231

JUN 04 2002

Technology Center 2100

Sir:

Attached hereto please find certified copies of applicant's Japanese applications as follows:

Japanese Patent Application No. 2000-133957 filed May 2, 2000

Japanese Patent Application No. 2000-103743 filed April 2, 2001

Applicant requests the benefit of said May 2, 2000 and April 2, 2001 filing dates for priority purposes pursuant to the provisions of 35 USC 119.

Respectfully submitted,

Louis Woo, RN 31,730
Law Offices of Louis Woo
1901 North Fort Myer Drive, Suite 501
Arlington, VA 22209
(703) 522-8872

Date:

May 31 2002



日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2000年 5月 2日

出 願 番 号
Application Number: 特願2000-133957

出 願 人
Applicant (s): 日本ビクター株式会社

RECEIVED

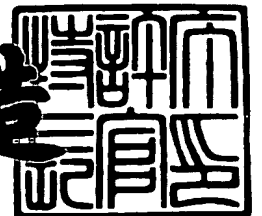
JUN 04 2002

Technology Center 2100

2001年 4月13日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3028719

【書類名】 特許願

【整理番号】 412000346

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 日本ビ
クター株式会社内

【氏名】 大石 剛士

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【代理人】

【識別番号】 100093067

【弁理士】

【氏名又は名称】 二瓶 正敬

【手数料の表示】

【予納台帳番号】 039103

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9004770

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証方法、コンテンツ送信側機器、コンテンツ受信側機器、認証システム

【特許請求の範囲】

【請求項 1】 コンテンツ送信側機器とコンテンツ受信側機器とが伝送媒体を介して接続され、前記コンテンツ送信側機器から前記コンテンツ受信側機器にコンテンツを送信するため、前記コンテンツ送信側機器が前記コンテンツ受信側機器の認証を行う第 1 及び第 2 のプロセスを有する認証方法であって、

前記第 1 のプロセスが、

- ・ 前記コンテンツ受信側機器を管理する第 1 及び第 2 の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第 1 の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第 2 の管理機関に付与される識別情報とが結合され、この結合情報に前記第 1 の管理機関に付与される署名が付加された情報を前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信するステップと、

- ・ 前記コンテンツ送信側機器が前記署名が付加された情報を受信するステップと、

- ・ 前記コンテンツ送信側機器が前記署名が付加された情報に含まれる前記コンテンツ受信側機器の前記証明情報を認証するステップと、

- ・ 前記コンテンツ送信側機器が前記コンテンツ受信側機器の前記証明情報を参照して、前記署名を認証するステップと、

- ・ 前記コンテンツ送信側機器が前記コンテンツ受信側機器の前記識別情報を記録手段に記録するステップとを有し、

前記第 1 のプロセスに続く前記第 2 のプロセスにおいて、

- ・ 前記コンテンツ受信側機器の前記識別情報を前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信するステップと、

- ・ 前記コンテンツ送信側機器が前記第 2 のプロセスで送信されたコンテンツ受信側機器の前記識別情報を受信するステップと、

- ・ 前記コンテンツ送信側機器が前記記録手段に記録された前記コンテンツ受信

側機器の前記識別情報と前記第 2 のプロセスで前記コンテンツ送信側機器が受信した前記コンテンツ受信側機器の前記識別情報とを照合するステップとを、
有する認証方法。

【請求項 2】 前記コンテンツ受信側機器の前記証明情報が前記コンテンツ受信側機器の信頼度情報を有することを特徴とする請求項 1 記載の認証方法。

【請求項 3】 伝送媒体を介してコンテンツ受信側機器と接続可能であり、前記コンテンツ受信側機器からコンテンツを受信するため、前記コンテンツ受信側機器の認証を行うコンテンツ送信側機器であって、

前記コンテンツ受信側機器を管理する第 1 及び第 2 の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第 1 の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第 2 の管理機関に付与される識別情報とが結合され、この結合情報に前記第 1 の管理機関に付与される署名が付加された情報、又は第 2 の管理機関により管理されている前記コンテンツ受信側機器の前記識別情報を前記コンテンツ受信側機器から受信する受信手段と、

前記コンテンツ受信側機器の前記証明情報、又は前記コンテンツ受信側機器の前記証明情報を認証した結果を用いて前記署名を認証する手段と、

前記コンテンツ受信側機器の前記識別情報を記録するための記録手段と、

前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と、前記受信した前記コンテンツ受信側機器の前記識別情報とを照合する照合手段とを、
有するコンテンツ送信側機器。

【請求項 4】 前記コンテンツ受信側機器の前記証明情報が前記コンテンツ受信側機器の信頼度情報を有することを特徴とする請求項 3 記載のコンテンツ送信側機器。

【請求項 5】 伝送媒体を介してコンテンツを送信するコンテンツ送信側機器と接続可能であり、前記コンテンツ送信側機器から前記コンテンツを受信するため、前記コンテンツ送信側機器の認証を受けるコンテンツ受信側機器であって、

前記コンテンツ受信側機器を管理する第 1 及び第 2 の管理機関が存在するとき

、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第 1 の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第 2 の管理機関に付与される識別情報とをあらかじめ格納する格納手段と、

前記格納手段にそれぞれ格納されている前記コンテンツ受信側機器の証明情報と前記コンテンツ受信側機器の識別情報とが結合され前記第 1 の管理機関に付与される署名が付加された情報、又は前記コンテンツ受信側機器の識別情報を前記コンテンツ送信側機器に送信する送信手段を、

有するコンテンツ受信側機器。

【請求項 6】 前記コンテンツ受信側機器の前記証明情報が前記コンテンツ受信側機器の信頼度情報を有することを特徴とする請求項 5 記載のコンテンツ受信側機器。

【請求項 7】 コンテンツ送信側機器からコンテンツを受信するコンテンツ受信側機器と、前記コンテンツ受信側機器にコンテンツを送信するため、第 1 及び第 2 のプロセスにより前記コンテンツ受信側機器の認証を行うコンテンツ送信側機器と、前記コンテンツ受信側機器と前記コンテンツ送信側機器とを接続する伝送媒体とを有する認証システムであって、

前記第 1 のプロセスで、前記コンテンツ受信側機器を管理する第 1 及び第 2 の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第 1 の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第 2 の管理機関に付与される識別情報とが結合され、この結合情報に前記第 1 の管理機関に付与される署名が付加された情報が前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信され、前記コンテンツ送信側機器で受信された前記コンテンツ受信側機器の前記証明情報が前記コンテンツ送信側機器で認証され、前記コンテンツ受信側機器の前記証明情報が参照されて前記署名が認証され、前記コンテンツ受信側機器の前記識別情報が前記コンテンツ送信側機器の記録手段に記録され、

前記第 1 のプロセスに続く前記第 2 のプロセスで、前記コンテンツ受信側機器の前記識別情報が前記コンテンツ受信側機器から前記コンテンツ送信側機器に送

信され、前記コンテンツ送信側機器で、前記コンテンツ送信側機器の前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と前記第 2 のプロセスで前記コンテンツ送信側機器に受信された前記コンテンツ受信側機器の前記識別情報とが照合される認証システム。

【請求項 8】 前記コンテンツ受信側機器の前記証明情報が前記コンテンツ受信側機器の信頼度情報を有することを特徴とする請求項 7 記載の認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル映像信号又はデジタル音声信号からなるコンテンツを、コンテンツ送信側機器からコンテンツ受信側機器に送信するため、コンテンツ送信側機器がコンテンツ受信側機器の認証を行う認証方法、コンテンツ送信側機器、コンテンツ受信側機器、認証システムであって、特に、デジタルインターフェイスを介してデバイス間で伝送する際に、データの改変や複製が行われる可能性のある機器への伝送を排除するために好適な技術に関する。

【0002】

【従来の技術】

IEEE 1394 などのデジタルインターフェイスが実用化されており、従来、このデジタルインターフェイスを用いてコンテンツを伝送する場合、コンテンツを不正に盗取されて著作権が侵害されるのを防ぐために、暗号化を含むコンテンツ保護プロセスが行われている。このプロセスでは、コンテンツ受信側機器の ID がコンテンツ送信側機器に送られ、この ID の確認を行いながら伝送が行われる。ところが、これだけではいったんコンテンツ受信側機器にコンテンツが取り込まれてしまうと、コンテンツ受信後のコンテンツの管理はコンテンツ受信側機器に任されてしまうため、コンテンツ受信側機器においてコンテンツの改変や複製を自由に行い得る機器であった場合には、著作権の侵害が容易に行われてしまうという問題があった。

【0003】

これに対して、本発明者らは、特願平 2 0 0 0 - 7 9 1 1 2 号、特願平 2 0 0 0 - 0 5 7 7 8 5 号において、コンテンツ伝送前にコンテンツ受信側機器からコンテンツ送信側機器にコンテンツ受信側機器の信頼度を送信し、その信頼度を評価することによって、コンテンツ送信側機器がコンテンツの伝送を行うか否かを決定できるシステムを提案している。

【0 0 0 4】

【発明が解決しようとする課題】

コンテンツ送信側機器からコンテンツ受信側機器にコンテンツを送信するため、コンテンツ送信側機器がコンテンツ受信側機器の認証を行う際に、例えば認証プロセスがただ 1 つのみの場合や複数の認証プロセスが独立して存在する場合、認証の途中やコンテンツの送信の途中で、例えば正当なコンテンツ受信側機器（シンクデバイス）が不当なコンテンツ受信側機器（シンクデバイス）に変わったり、接続のための伝送媒体（接続ケーブル）から情報が盗取されたりする場合には、本来送ってはならない不当なコンテンツ受信側機器にコンテンツが送られてしまうことがある。また、例えばコンテンツ送信側機器が正当なコンテンツ受信側機器 α の認証を行っても、認証が完了してコンテンツの送信が行われるとき、不正なコンテンツ受信側機器 β が正当なコンテンツ受信側機器 α のふりをして、コンテンツの受信をしてしまうこともある。

【0 0 0 5】

本発明は、コンテンツ送信側機器からコンテンツ受信側機器にコンテンツを送信する際、コンテンツ送信側機器から所望のコンテンツ受信側機器に、コンテンツを盗取されずに確実に送信可能となるよう認証を行う認証方法、コンテンツ送信側機器、コンテンツ受信側機器、認証システムを提供することを目的とする。

【0 0 0 6】

【課題を解決するための手段】

本発明は、上記目的を達成するため、まず第 1 のプロセスにおいて、コンテンツ受信側機器が第 1 の管理機関からライセンスを受けている証明となる証明情報と、第 2 の管理機関により管理されている識別情報とが結合されて署名が付加された情報をコンテンツ送信側機器に送信し、コンテンツ送信側機器が証明情報を

認証し、さらにその証明情報を参照して署名を認証し、識別情報を保存し、続く第2のプロセスにおいて、再びコンテンツ受信側機器が第2の管理機関に管理されている識別情報をコンテンツ送信側機器に送信し、その識別情報をコンテンツ送信側機器で受信して、第1のプロセスで保存された識別情報と照合することにより、コンテンツ送信側機器がコンテンツ受信側機器を認証する。

【0007】

すなわち、本発明によれば、コンテンツ送信側機器とコンテンツ受信側機器とが伝送媒体を介して接続され、前記コンテンツ送信側機器から前記コンテンツ受信側機器にコンテンツを送信するため、前記コンテンツ送信側機器が前記コンテンツ受信側機器の認証を行う第1及び第2のプロセスを有する認証方法であって

前記第1のプロセスが

- ・前記コンテンツ受信側機器を管理する第1及び第2の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第1の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第2の管理機関に付与される識別情報とが結合され、この結合情報に前記第1の管理機関に付与される署名が付加された情報を前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信するステップと、

- ・前記コンテンツ送信側機器が前記署名が付加された情報を受信するステップと、

- ・前記コンテンツ送信側機器が前記署名が付加された情報に含まれる前記コンテンツ受信側機器の前記証明情報を認証するステップと、

- ・前記コンテンツ送信側機器が前記コンテンツ受信側機器の前記証明情報を参照して、前記署名を認証するステップと、

- ・前記コンテンツ送信側機器が前記コンテンツ受信側機器の前記識別情報を記録手段に記録するステップとを有し、

前記第1のプロセスに続く前記第2のプロセスにおいて、

- ・前記コンテンツ受信側機器の前記識別情報を前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信するステップと、

- ・前記コンテンツ送信側機器が前記第2のプロセスで送信されたコンテンツ受信側機器の前記識別情報を受信するステップと、

- ・前記コンテンツ送信側機器が前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と前記第2のプロセスで前記コンテンツ送信側機器が受信した前記コンテンツ受信側機器の前記識別情報とを照合するステップとを、
有する認証方法が提供される。

【0008】

また、本発明によれば、伝送媒体を介してコンテンツ受信側機器と接続可能であり、前記コンテンツ受信側機器からコンテンツを受信するため、前記コンテンツ受信側機器の認証を行うコンテンツ送信側機器であって、

前記コンテンツ受信側機器を管理する第1及び第2の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第1の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第2の管理機関に付与される識別情報とが結合され、この結合情報に前記第1の管理機関に付与される署名が付加された情報、又は第2の管理機関により管理されている前記コンテンツ受信側機器の前記識別情報を前記コンテンツ受信側機器から受信する受信手段と、

前記コンテンツ受信側機器の前記証明情報、又は前記コンテンツ受信側機器の前記証明情報を認証した結果を用いて前記署名を認証する手段と、

前記コンテンツ受信側機器の前記識別情報を記録するための記録手段と、

前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と、前記受信した前記コンテンツ受信側機器の前記識別情報とを照合する照合手段とを、
有するコンテンツ送信側機器が提供される。

【0009】

また、本発明によれば、伝送媒体を介してコンテンツを送信するコンテンツ送信側機器と接続可能であり、前記コンテンツ送信側機器から前記コンテンツを受信するため、前記コンテンツ送信側機器の認証を受けるコンテンツ受信側機器であって、

前記コンテンツ受信側機器を管理する第1及び第2の管理機関が存在するとき

、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第 1 の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第 2 の管理機関に付与される識別情報とをあらかじめ格納する格納手段と、

前記格納手段にそれぞれ格納されている前記コンテンツ受信側機器の証明情報と前記コンテンツ受信側機器の識別情報とが結合され前記第 1 の管理機関に付与される署名が付加された情報、又は前記コンテンツ受信側機器の識別情報を前記コンテンツ送信側機器に送信する送信手段を、

有するコンテンツ受信側機器が提供される。

【 0 0 1 0 】

また、本発明によれば、コンテンツ送信側機器からコンテンツを受信するコンテンツ受信側機器と、前記コンテンツ受信側機器にコンテンツを送信するため、第 1 及び第 2 のプロセスにより前記コンテンツ受信側機器の認証を行うコンテンツ送信側機器と、前記コンテンツ受信側機器と前記コンテンツ送信側機器とを接続する伝送媒体とを有する認証システムであって、

前記第 1 のプロセスで、前記コンテンツ受信側機器を管理する第 1 及び第 2 の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第 1 の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第 2 の管理機関に付与される識別情報とが結合され、この結合情報に前記第 1 の管理機関に付与される署名が付加された情報が前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信され、前記コンテンツ送信側機器で受信された前記コンテンツ受信側機器の前記証明情報が前記コンテンツ送信側機器で認証され、前記コンテンツ受信側機器の前記証明情報が参照されて前記署名が認証され、前記コンテンツ受信側機器の前記識別情報が前記コンテンツ送信側機器の記録手段に記録され、

前記第 1 のプロセスに続く前記第 2 のプロセスで、前記コンテンツ受信側機器の前記識別情報が前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信され、前記コンテンツ送信側機器で、前記コンテンツ送信側機器の前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と前記第 2 のプロセス

で前記コンテンツ送信側機器に受信された前記コンテンツ受信側機器の前記識別情報とが照合される認証システムが提供される。

【0011】

また、上記の認証方法、コンテンツ送信側機器、コンテンツ受信側機器、認証システムのそれぞれにおいて、コンテンツ受信側機器の証明情報がコンテンツ受信側機器の信頼度情報を有することは、本発明の好ましい態様である。

【0012】

【発明の実施の形態】

以下、図面を参照しながら、本発明に係る実施の形態に関して説明する。図1は、本発明に係るソースデバイス（コンテンツ送信側機器）からシンクデバイス（コンテンツ受信側機器）にコンテンツを送信するために行われる手順の一実施形態を示すフローチャートである。本発明では、後述する第1のプロセス（ステップS1）、第2のプロセス（ステップS2）、鍵交換プロセス（ステップS3）の認証プロセスを行うことによって、ソースデバイス（コンテンツ送信側機器）からシンクデバイス（コンテンツ受信側機器）にコンテンツを確実に送信する。

【0013】

図9は、本発明に係るソースデバイス及びシンクデバイスを構成する手段を示す模式図である。ソースデバイス1とシンクデバイス2とは、IEEE1394などのデジタルインターフェイスによって接続されている。ソースデバイス1は、送信手段3、受信手段4、演算手段5、格納手段6、メモリ7、照合手段8を有している。一方、シンクデバイス2は、送信手段3、受信手段4、演算手段5、格納手段6、メモリ7を有している。送信手段3は、接続された機器に対して情報を送信する手段である。受信手段4は、接続された機器から情報を受信する手段である。演算手段5は、あるデータに対して、別のデータを用いて演算を行う手段であり、署名の作成や認証に用いられる。格納手段6は、データを格納しておく手段である。メモリ7は、送受信や演算などを行うときに一時的にデータを記録するための記録手段である。照合手段8は、2つの情報を比較して、それらの情報が一致しているか否かを照合する手段である。また、図示省略している

が、ソースデバイス 1 及びシンクデバイス 2 はそれぞれ CPU を有しており、この CPU によって各手段の動作が制御されている。

【 0 0 1 4 】

図 8 は、ソースデバイス及びシンクデバイスが有している格納手段に格納されている情報を示す模式図である。ソースデバイス 1 の格納手段 6 には、公開鍵 X pub、公開鍵 Z pub、公開鍵 W 2 pub、秘密鍵 W 2 prv が格納されている。一方、シンクデバイス 2 の格納手段 6 には、公開鍵 Y pub (図 1 2 に図示) を含む A org 証明情報、秘密鍵 Y prv、第 2 のプロセス用 ID、公開鍵 W 1 pub (図 1 2 に図示) を含む B org 証明情報、秘密鍵 W 1 prv、公開鍵 X pub、公開鍵 Z pub が格納されている。

【 0 0 1 5 】

第 1 のプロセスでは、ソースデバイス 1 の格納手段 6 に格納されている公開鍵 X pub が用いられる。また、シンクデバイス 2 の格納手段 6 に格納されている第 2 のプロセス用 ID、秘密鍵 Y prv、A org 証明情報が用いられる。公開鍵 X pub は、第 1 のプロセスの管理機関 A org にライセンスを与えられた全てのデバイスが有する公開鍵である。この公開鍵 X pub は、秘密鍵 X prv と対になっている。第 2 のプロセス用 ID は、管理機関 B org から与えられた各デバイスに固有の識別子であり、この第 2 のプロセス用 ID によって、各デバイスの識別が可能となる。秘密鍵 Y prv は、そのデバイスから外部に出されることのない秘密鍵であり、署名 sign A 1 を作成するのに用いられる。この秘密鍵 Y prv は、公開鍵 Y pub と対になっている。

【 0 0 1 6 】

公開鍵 Y pub は、各デバイスに固有の鍵である秘密鍵 Y prv を用いて作成された署名を検証するための個々のデバイスに固有の鍵で、管理機関 A org により与えられている。A org 証明情報は、あらかじめ管理機関 A org により与えられており、この公開鍵 Y pub を含む情報に対して、秘密鍵 X prv を用いて演算が行われ、署名 sign A 1 が付加された情報である。この A org 証明情報として、例えば管理機関 A org がライセンシーにのみ与える公開情報を利用することも可能である。なお、秘密鍵 X prv は、管理機関 A org のみによって管理されるものであり、管理機

関Aorg以外の第3者が署名signA1を含むAorg証明情報を作成することはできない。

【0017】

このAorg証明情報と第2のプロセス用IDとが結合された情報を情報Aと呼ぶことにする。情報Aに関しては、Aorg証明情報と第2のプロセス用IDとに一方関数を作用させた結果を結合させて、この結合情報を情報Aとするのが好適である。また、この情報Aに対して、あらかじめシンクデバイス2が持っている秘密鍵Yprvを用いて演算が行われる。この情報Aは、あらかじめ一括してシンクデバイス2に付与されているのが好適である。また、署名signA2が付加された情報を情報Bと呼ぶことにする。この情報Bが、後述する第1のプロセスにおいて、シンクデバイス2からソースデバイス1に送信される。署名signA1の情報を参照することで、秘密鍵Xprvを用いて作成された署名signA1が付加された公開鍵Y1pubが改ざんされているか否かを判断することが可能となる。また、署名signA2の情報を参照することで、秘密鍵Yprvを用いて作成された署名signA2が付加されている情報Aが改ざんされているか否かを判断することが可能となる。

【0018】

第2のプロセス及び鍵交換プロセスでは、ソースデバイス1の格納手段6に格納されている秘密鍵W2prv、公開鍵Zpub、公開鍵W2pubが用いられる。また、シンクデバイス2の格納手段6に格納されている秘密鍵W1prv、第2のプロセス用ID、公開鍵W1pub（図12に図示）を含むBorg証明情報、公開鍵Zpubが用いられる。公開鍵Zpubは、管理機関Borgにライセンスを与えられた全てのデバイスが有する公開鍵である。この公開鍵Zpubは、秘密鍵Zprvと対になっている。なお、秘密鍵Zprvは、管理機関Borgのみによって管理されるものであり、管理機関Borg以外の第3者が署名signB1を含むBorg証明情報を作成することはできない。

【0019】

第2のプロセス用IDと公開鍵W1pubとが結合された情報を情報Cと呼び、この情報Cに対して秘密鍵Zprvを用いて演算が行われ、署名signB1が付加さ

れた情報をB org証明情報と呼ぶことにする。このB org証明情報が、後述する第2のプロセスにおいて、シンクデバイス2からソースデバイス1に送信される。署名signB 1の情報を参照することで、秘密鍵Z prvを用いて作成された署名signB 1が付加されたB org証明情報が改ざんされているか否かを判断することが可能となる。

【0020】

公開鍵W 1 pub、公開鍵W 2 pub、秘密鍵W 1 prv、秘密鍵W 2 prvは鍵交換プロセスで用いられる鍵であり、後述のように、第2のプロセスで公開鍵W 1 pubと公開鍵W 2 pubがソースデバイス1とシンクデバイス2との間で交換される。公開鍵W 1 pub及び公開鍵W 2 pubは、管理機関B orgによってライセンスが与えられた全ての機器が有する鍵であり、秘密鍵W 1 prv及び秘密鍵W 2 prvは、管理機関B orgによって各デバイスに対して与えられた固有の鍵である。

【0021】

<第1のプロセス>

図1は、本発明に係る第1のプロセスの一実施形態におけるソースデバイスの動作を示すフローチャートである。ステップS 1 0 1において、受信手段4によりシンクデバイス2から情報Bを受信する。受信するまでは待ち状態になっている。図12(a)は、情報Bの構成を示す模式図である。情報Bはシンクデバイス2の格納手段6に格納されている情報により構成されており、A org証明情報と第2のプロセス用IDとが結合された情報Aに対して、あらかじめシンクデバイス2が持っている秘密鍵Y prvを用いて演算が行われ、署名signA 2が付加された情報である。

【0022】

ステップS 1 0 3において、ステップS 1 0 1で受信した情報Bに含まれる公開鍵Y pubが改ざんされていないことを確認する。例えば、公開鍵Y pubが付加されている署名signA 1の一部は元々の公開鍵Y pubのデータから派生したものであり、ソースデバイス1において、ステップS 1 0 1で受信した情報B内の公開鍵Y pubを含む情報に対して、あらかじめソースデバイス1が持っている公開鍵X pubを用いて演算手段5により演算を行い、この演算結果が上記の署名signA

1の一部と同一であることを確認することによって、公開鍵 Y_{pub} が改ざんされていないことが証明される。改ざんされていないことが確認できない場合は、図 11 に示すステップ S 199 において、認証は失敗となり処理を終了する。なお、フローチャートに示されている①は、図 11 の①に繋がっている。

【0023】

次に、ステップ S 105 において、ステップ S 101 で受信した情報 B に含まれる第 2 のプロセス用 ID が改ざんされていないことを確認する。例えば、第 2 のプロセス用 ID を含む情報 A に付加されている署名 $signA_2$ の一部は元々の情報 A のデータから派生したものであり、ソースデバイス 1 において、ステップ S 101 で受信した情報 B 内の情報 A に対して、ステップ S 103 で改ざんされていないことを確認したソースデバイス 1 が持っている公開鍵 Y_{pub} を用いて演算手段 5 により演算を行い、この演算結果が上記の署名 $signA_2$ の一部と同一であることを確認することによって、情報 A 及び情報 A 内の第 2 のプロセス用 ID が改ざんされていないことが証明される。改ざんされていないことが確認できない場合は、図 11 に示すステップ S 199 において、認証は失敗となり処理を終了する。

【0024】

ステップ S 107 において、ステップ S 101 で受信した情報 B に含まれる第 2 のプロセス用 ID をメモリ 7 に記録する。保存された第 2 のプロセス用 ID は、後述の認証プロセス（第 2 のプロセス）において用いられる。次に、ステップ S 109 において、ステップ S 101 で受信した情報 B の認証に成功したことを送信手段 3 によりシンクデバイス 2 に通知する。以上が第 1 のプロセスにおけるソースデバイス 1 のフローチャートである。

【0025】

次に、シンクデバイス 2 の動作に関して説明する。図 2 は、本発明に係る第 1 のプロセスの一実施形態におけるシンクデバイスの動作を示すフローチャートである。ステップ S 201 において、送信手段 3 によりソースデバイス 1 に情報 B を送信する。情報 B は、A org 証明情報と第 2 のプロセス用 ID とが結合された情報 A に対して、あらかじめシンクデバイス 2 が持っている秘密鍵 Y_{prv} を用い

て演算が行われ、署名signA 2が付加された情報であるが、この署名signA 2の付加をシンクデバイス内で行うことも可能であり、また、あらかじめ署名signA 2が付加された情報を格納手段に格納しておくことも可能である。情報Bを送信した後は、ステップS 2 0 3でソースデバイス1から認証の成功の通知を受信するまで待ち状態となる。以上が第1のプロセスにおけるシンクデバイスのフローチャートである。

【 0 0 2 6 】

また、前述した特願平 2 0 0 0 - 7 9 1 1 2 号、特願平 2 0 0 0 - 0 5 7 7 8 5 号に記載されている認証システムを利用して、ソースデバイス1にシンクデバイス2の信頼度情報を送信するときに、ソースデバイス1への信頼度情報の送信とステップS 2 0 1での公開鍵Y pub、第2のプロセス用IDの送信を同時に行うことも可能である。信頼度情報は所定の管理機関から与えられる情報であり、この信頼度情報を管理する管理機関と第1のプロセスの管理機関A orgが同一の場合には、公開鍵Y pubと信頼度情報とが結合されて、1つの署名で裏書きしたものをA org証明情報とすることも可能である。

【 0 0 2 7 】

この場合、ソースデバイス1では、ステップS 1 0 5とステップS 1 0 7の間に、シンクデバイス2の信頼度がコンテンツの送信が可能な信頼度か否かを判断するステップが付加されることが好ましい。この場合、コンテンツの伝送を行ってもいいと判断する基準となる信頼度をソースデバイス1が有しており、この基準となる信頼度よりもシンクデバイス2の信頼度のほうが低い場合は、ソースデバイス1からのコンテンツの送信は不可能と判断され、処理を終了する。

【 0 0 2 8 】

また、上記第1のプロセスにおいて、ステップS 1 0 9でソースデバイス1からシンクデバイス2に認証の成功を通知する代わりに、ソースデバイス1が持っているA org証明情報をシンクデバイス2に送信するステップを付加して、シンクデバイス2においてもソースデバイス1の認証を行うようにすることも可能である。この場合、シンクデバイス2が認証側、ソースデバイス1が被認証側となって、シンクデバイス2でステップS 1 0 1からステップS 1 0 7の動作が、ソ

ースデバイス1でステップS 2 0 1からS 2 0 3の動作が行われる。また、この場合、ソースデバイス1も管理機関A orgからA org証明情報が与えられており、さらに、秘密鍵Y prvを有していて、署名signA 2の作成が可能である必要がある。これらのステップにより、不当なソースデバイス1が、正当なシンクデバイス2に対して何度も何度も情報提供を要求して暗号解読をしようという操作を途中で停止させることが可能となり、ソースデバイス1及びシンクデバイス2により構成されるシステム全体の破壊に対する強度を強めることが可能となる。

【 0 0 2 9 】

<第2のプロセス>

図3は、本発明に係る第2のプロセスの一実施形態におけるソースデバイスの動作を示すフローチャートである。ステップS 1 1 1において、シンクデバイス2からB org証明情報を受信手段4により受信する。図1 2 (b)は、B org証明情報の構成を示す模式図である。B org証明情報は、第2のプロセス用IDと公開鍵W 1 pubとが結合された情報Cに署名signB 1が付加されたものである。前述した情報Aの場合と同様、第2のプロセス用IDと公開鍵W 1 pubとの結合は、単にそれぞれの情報をつなぐだけでもよく、また、これらの情報に一方関数を作用させた結果を結合させてもよい。シンクデバイス2からB org証明情報を受信できず、所定の時間、待ち状態が続いた場合はタイムアウトとなり、図1 1に示すステップS 1 9 9において、処理を終了する。ステップS 1 1 3において、ステップS 1 1 1で受信したB org証明情報内の情報C（第2のプロセス用ID及び公開鍵W 1 pub）が改ざんされていないことを確認する。例えば、情報Cに付加されている署名signB 1の一部は元々の情報Cから派生したものであり、ソースデバイス1において、ステップS 1 1 1で受信したB org証明情報内の情報Cに対して、あらかじめソースデバイス1が持っている公開鍵Z pubを用いて演算手段5により演算を行い、この演算結果が上記の署名signB 1の一部と同一であることを確認することによって、情報Cが改ざんされていないことが証明される。改ざんされていないことが確認できない場合は、図1 1に示すステップS 1 9 9において、認証は失敗となり処理を終了する。

【 0 0 3 0 】

ステップS115において、ステップS107でメモリに保存された第2のプロセス用IDと、ステップS111で受信したBorg証明情報に含まれる第2のプロセス用IDとが一致しているか否かを照合手段8により照合する。両者が一致した場合、ソースデバイス1はシンクデバイス2を正常に認証できたとして、コンテンツの伝送の手順が行われる。一方、両者が異なる場合、図11に示すステップS199において、認証は失敗となり処理を終了する。ステップS115で認証が成功した場合、ステップS116において、送信手段3により公開鍵W2 pubをシンクデバイス2に送信する。このステップS116での公開鍵W2 pubの送信の際、ステップS111でシンクデバイス2から受信した情報のように公開鍵W2 pubをソースデバイス1の第2のプロセス用IDと結合して、さらに署名を付加した情報を送信してもよい。以上が第2のプロセスにおけるソースデバイス1のフローチャートである。

【0031】

一方、第2のプロセスにおけるシンクデバイス2の動作は以下の通りである。図4は、本発明に係る第2のプロセスの一実施形態におけるシンクデバイスの動作を示すフローチャートである。ステップS205において、送信手段3によりBorg証明情報をソースデバイス1に送信する。Borg証明情報には、第2のプロセス用IDと公開鍵W1 pubが含まれている。次に、ステップS206において、ステップS116でソースデバイス1から送信された公開鍵W2 pubを受信手段4により受信する。ソースデバイス1でBorg証明情報の認証が成功した場合、鍵交換プロセスが行われるまで待ち状態となる。

【0032】

ステップS206で受信した公開鍵W2 pubがソースデバイス1の第2のプロセス用IDと結合されて、さらに署名が付加されている情報の場合、ソースデバイス1で行われたステップS111からS115までの認証プロセスをシンクデバイス2で行うことも可能である。これにより、ソースデバイス1及びシンクデバイス2のそれぞれにおいて、第2のプロセスによる相手機器の認証が可能となる。以上が第2のプロセスにおけるシンクデバイス2のフローチャートである。このようにして、第2のプロセスにおいて、公開鍵W1 pubと公開鍵W2 pubがソ

ースデバイス1とシンクデバイス2との間で交換される。

【0033】

＜鍵交換プロセス＞

一方、コンテンツの伝送の際に行われる鍵交換プロセスは以下の通りである。図5は、鍵交換プロセスにおけるソースデバイスの動作を示すフローチャートである。ステップS117において、ソースデバイス1が持っている所定のデータに対して、あらかじめソースデバイス1が持っている秘密鍵W2_{prv}を用いて演算手段5により演算を行い、データを生成する。ステップS119において、送信手段3により生成されたデータをシンクデバイス2に送信する。ステップS121において、受信手段4によりシンクデバイス2からデータを受信する。このデータは、シンクデバイス2において、後述するステップS215（図6に記載）で生成されたデータである。ステップS123において、シンクデバイス2から受信したデータに対して、先の過程でシンクデバイス2から受信した公開鍵W1_{pub}を用いて演算手段5により演算を行い、この結果、暗号化鍵Uが生成される。ステップS125において、この暗号化鍵Uを、シンクデバイス2のメモリ7に保存する。

【0034】

図6は、鍵交換プロセスにおけるシンクデバイスの動作を示すフローチャートである。ステップ207において、ソースデバイス1からデータを受信手段4により受信する。このデータは、ソースデバイス1において、ステップS119で生成されたデータである。ステップS209において、ソースデバイス1から受信したデータに対して、ステップS206でソースデバイス1から受信した公開鍵W2_{pub}を用いて演算手段5により演算を行い、この結果、暗号化鍵Vが生成される。ステップS211において、この暗号化鍵Vをシンクデバイス2のメモリ7に保存する。ステップS213において、シンクデバイス2が持っている所定のデータに対して、あらかじめシンクデバイス2が持っている秘密鍵W1_{prv}を用いて演算手段5により演算を行い、データを生成する。ステップS215において、送信手段3により生成されたデータをソースデバイス1に送信する。

【0035】

この鍵交換プロセスにより、ソースデバイス1、シンクデバイス2は、それぞれ暗号化鍵U、暗号化鍵Vを有することになる。この暗号化鍵Uと暗号化鍵Vとは同一のものである。したがって、コンテンツの送信の際に、ソースデバイス1側で暗号化鍵Uを用いてコンテンツを暗号化すれば、暗号化されたコンテンツの復号が可能であるシンクデバイス2、すなわち暗号化鍵Vを有するシンクデバイス2だけが、受信したコンテンツの復号を行うことができる。このようにして、ソースデバイス1から特定のシンクデバイス2にコンテンツの送信を行うことが可能となる。

【0036】

また、図13は、上記第1のプロセス、第2のプロセス、鍵交換プロセスにおけるソースデバイス及びシンクデバイスの動作をまとめて示すタイムチャートである。このタイムチャートは、上記の図1から図6までのフローチャートをまとめたものであり、図の左側はソースデバイス1、図の右側はシンクデバイス2、両者の間を結ぶ線はソースデバイス1とシンクデバイス2との間の情報の伝送を示している。

【0037】

次に、図13に示した認証プロセスの全体の流れを参照して、正当なシンクデバイス2になりすまして、不正なシンクデバイス2がコンテンツを受信しようと企てる“なりすまし”の様々な状況を想定して説明する。図7は、コンテンツの伝送の際に考えられる不正なシンクデバイス2を排除する過程を示す模式図である。今、管理機関Aorgからのライセンスを受けていない不当なシンクデバイス2が、正当なシンクデバイス2になりすまして、コンテンツを受けようとしている場合を考える。ただし不当なシンクデバイス2は管理機関Borgのライセンスは受けているものとする。

【0038】

不当なシンクデバイス2が、正当なシンクデバイス2が第1のプロセスで送った情報を盗取して、ソースデバイス1から認証を得ようとする場合、

(A1) 同じものを送る場合。

第2のプロセス用IDを含むAorg証明情報は、正当なシンクデバイス2のも

のである。したがって、不当なシンクデバイス 2 がこの情報を送った場合、ソースデバイス 1 は、正当なシンクデバイス 2 から送信されたものと判断して、不当なシンクデバイス 2 の“なりすまし”は見破られない。

(A 2) 第 2 のプロセス用 ID を不当なシンクデバイス 2 のものに変えて送る場合。

秘密鍵 Y_{prv} が正当なシンクデバイス 2 と異なるため、署名 $\text{signA } 2$ が正当なシンクデバイス 2 のものとは異なってしまう、不当なシンクデバイス 2 であることが明らかとなる。

【 0 0 3 9 】

上記 (A 1) の場合、不当なシンクデバイス 2 は、第 1 のプロセスで認証される。このように第 1 のプロセスで認証された不当なシンクデバイス 2 は、再び第 2 のプロセスにおいて認証される必要がある。

(B 1) 正当なシンクデバイス 2 の B_{org} 証明情報を盗取して、同じものを送る場合。

B_{org} 証明情報の第 2 のプロセス用 ID 及び公開鍵 $W 1_{\text{pub}}$ は正当なシンクデバイス 2 のものである。したがって、ステップ S 1 1 5 において、ステップ S 1 0 7 で保存した第 2 のプロセス用 ID とステップ S 1 1 1 で受信した B_{org} 証明情報内の第 2 のプロセス用 ID との照合を行った場合、両者は一致するので、不当なシンクデバイス 2 の“なりすまし”は見破られない。

【 0 0 4 0 】

(B 2) 不当なシンクデバイス 2 の第 2 のプロセス用 ID が含まれるように B_{org} 証明情報を改ざんして送る場合。

不当なシンクデバイス 2 も管理機関 B_{org} のライセンスを受けているので、第 2 のプロセス用 ID の認証のみが行われるならば、認証されてしまう。しかし、本発明では、ステップ S 1 1 5 において、前もってステップ S 1 0 7 で保存した第 2 のプロセス用 ID とステップ S 1 1 1 で受信した B_{org} 証明情報内の第 2 のプロセス用 ID との照合を行い、両者が一致しないことを確かめるので、不当なシンクデバイス 2 の“なりすまし”であることが明らかとなる。

【 0 0 4 1 】

(B1)で認証された不当なシンクデバイス2も次の鍵交換プロセスにおいて、不当なシンクデバイス2であることが明らかになってしまう。鍵交換プロセスにおいて、ソースデバイス1に送信される秘密鍵W1 prvは不当なシンクデバイス2のものであるため、伝送するコンテンツを暗号化するときの暗号化鍵Vは正当なシンクデバイス2の公開鍵W1 pubと不当なシンクデバイス2の秘密鍵W1 prvを用いて作られることになってしまう。したがって、この暗号化鍵Vを用いてコンテンツを暗号化してソースデバイス1から送信しても、シンクデバイス2でコンテンツをデコードすることは不可能である。

【0042】

また、鍵交換プロセスの代わりに、ソースデバイス1からシンクデバイス2にコンテンツを送信しながら、所定の時間間隔ごとに第2のプロセスを行って、ステップS107でメモリに保存された第2のプロセス用IDと、ステップS111で受信したBorg証明情報に含まれる第2のプロセス用IDとが一致しているか否かを比較することも可能である。この方法でも、コンテンツの送信の途中で正当なシンクデバイス2から不当なシンクデバイス2にコンテンツが送信されてしまうことを防ぎ、所望の相手機器にのみコンテンツを送信することが可能となる。

【0043】

図10は、ソースデバイスとシンクデバイスの様々な接続形態を示す図である。上記実施形態では、ソースデバイス1とシンクデバイス2との接続形態は、図10(a)に示すようなIEEE1394による1対1の接続の他に、図10(c)に示す1対多が可能であり、また、図10(b)、図10(d)のようにインターネットなどのネットワークを介しての接続も可能である。

【0044】

また、コンテンツ送信側において、シンクデバイス2を認証する機能を有する認証装置を、シンクデバイス2にコンテンツの送信を行うコンテンツ送信装置から独立なものとするのが可能である。また、コンテンツ受信側においても同様に、ソースデバイス1に認証される機能を有する被認証装置を、ソースデバイス1からコンテンツを受信するコンテンツ受信装置から独立なものとするのが可

能である。

【 0 0 4 5 】

本発明によれば、[特許請求の範囲]の欄に記載された発明の他に、次のような発明が提供される。

(1) 前記証明情報が、前記結合情報に付加される前記署名を認証するために必要な情報の一部を有することを特徴とする請求項1又は2記載の認証方法。

(2) 前記証明情報が、前記第1の管理機関に著作権が存在する著作物を有することを特徴とする請求項1又は2記載の認証方法。

(3) 前記証明情報と前記識別情報とに対して、一方向関数を作用させて前記結合情報を生成するステップを有することを特徴とする請求項1又は2記載の認証方法。

(4) 前記証明情報を認証するステップにおいて、前記第1の管理機関がライセンスのみを与える公開情報を利用して、前記証明情報を認証することを特徴とする請求項1又は2記載の認証方法。

(5) 前記証明情報又は前記証明情報に含まれる署名認証のための情報が、前記コンテンツ受信側機器のそれぞれに関して異なるものであることを特徴とする請求項1又は2記載の認証方法。

(6) 前記証明情報が、前記第1の管理機関により一括してコンテンツ受信側機器に付与されていることを特徴とする請求項1又は2記載の認証方法。

(7) 前記第2のプロセスに続く認証プロセスとして、前記第2のプロセスで用いられた情報を利用して鍵交換プロセスを行うステップを有することを特徴とする請求項1又は2記載の認証方法。

【 0 0 4 6 】

(8) 前記証明情報が、前記結合情報に付加される前記署名を認証するために必要な情報の一部を有することを特徴とする請求項3又は4記載のコンテンツ送信側機器。

(9) 前記証明情報が、前記第1の管理機関に著作権が存在する著作物を有することを特徴とする請求項3又は4記載のコンテンツ送信側機器。

(10) 前記結合情報が、前記証明情報と前記識別情報とに対して、一方向関数

を作用させて生成されたものであることを特徴とする請求項3又は4記載のコンテンツ送信側機器。

(11) 前記署名を認証する手段において、前記第1の管理機関がライセンシーのみを与える公開情報を利用して、前記証明情報が認証されることを特徴とする請求項3又は4記載のコンテンツ送信側機器。

(12) 前記証明情報又は前記証明情報に含まれる署名認証のための情報が、前記コンテンツ受信側機器のそれぞれに関して異なるものであることを特徴とする請求項3又は4記載のコンテンツ送信側機器。

(13) 前記証明情報が、前記第1の管理機関により一括して付与されていることを特徴とする請求項3又は4記載のコンテンツ送信側機器。

(14) 前記コンテンツ受信側機器から受信した情報を利用して鍵交換プロセスを行うための手段を有することを特徴とする請求項3又は4記載のコンテンツ送信側機器。

【0047】

(15) 前記証明情報が、前記結合情報に付加される前記署名を認証するために必要な情報の一部を有することを特徴とする請求項5又は6記載のコンテンツ受信側機器。

(16) 前記証明情報が、前記第1の管理機関に著作権が存在する著作物を有することを特徴とする請求項5又は6記載のコンテンツ受信側機器。

(17) 前記結合情報が、前記証明情報と前記識別情報とに対して、一方向関数を作用させて生成されたものであることを特徴とする請求項5又は6記載のコンテンツ受信側機器。

(18) 前記証明情報又は前記証明情報に含まれる署名認証のための情報が、各機器に関してそれぞれ異なるものであることを特徴とする請求項5又は6記載のコンテンツ受信側機器。

(19) 前記証明情報が、前記第1の管理機関により一括して付与されていることを特徴とする請求項5又は6記載のコンテンツ受信側機器。

(20) 前記コンテンツ送信側機器から受信した情報を利用して鍵交換プロセスを行うための手段を有することを特徴とする請求項5又は6記載のコンテンツ受

信側機器。

【 0 0 4 8 】

(2 1) 前記証明情報が、前記結合情報に付加される前記署名を認証するために
必須な情報の一部を有することを特徴とする請求項 7 又は 8 記載の認証システム

(2 2) 前記証明情報が、前記第 1 の管理機関に著作権が存在する著作物を有す
ることを特徴とする請求項 7 又は 8 記載の認証システム。

(2 3) 前記結合情報が、前記証明情報と前記識別情報とに対して、一方向関数
を作用させて生成されたものであることを特徴とする請求項 7 又は 8 記載の認証
システム。

(2 4) 前記コンテンツ送信側機器が有する前記署名を認証する手段において、
前記第 1 の管理機関がライセンシーのみを与える公開情報を利用して、前記証明
情報が認証されることを特徴とする請求項 7 又は 8 記載の認証システム。

(2 5) 前記証明情報又は前記証明情報に含まれる署名認証のための情報が、前
記コンテンツ受信側機器のそれぞれに関して異なるものであることを特徴とする
請求項 7 又は 8 記載の認証システム。

(2 6) 前記証明情報が、前記第 1 の管理機関により一括して前記コンテンツ受
信側機器に付与されていることを特徴とする請求項 7 又は 8 記載の認証システム

(2 7) 前記コンテンツ送信側機器及び前記コンテンツ受信側機器が、前記第 2
のプロセスで用いられた情報を利用して前記第 2 のプロセスに続いて鍵交換プロ
セスを行うための手段を有することを特徴とする請求項 7 又は 8 記載の認証シス
テム。

【 0 0 4 9 】

【発明の効果】

本発明によれば、まず第 1 のプロセスにおいて、コンテンツ受信側機器（シン
クデバイス）が第 1 の管理機関からライセンスを受けている証明となる証明情報
と、第 2 の管理機関により管理されている識別情報とが結合されて、署名が付加
された情報をコンテンツ送信側機器（ソースデバイス）に送信し、コンテンツ送

信側機器が証明情報を認証し、さらにその証明情報を参照して署名を認証し、識別情報を保存し、続く第2のプロセスにおいて、再びコンテンツ受信側機器が第2の管理機関に管理されている識別情報をコンテンツ送信側機器に送信し、その識別情報をコンテンツ送信側機器で受信して、第1のプロセスで保存された識別情報と照合することにより、コンテンツ送信側機器がコンテンツ受信側機器を認証するので、第2のプロセス用IDや、管理機関Aorgからライセンスを受けている証明となる証明書によって守られた（改ざんの検出が可能となっている）信頼度情報と公開鍵（署名signA1に守られている）とペアになるべき第2プロセス用ID（署名signA2に守られている）が他者に改ざんされたりするのを防ぐことが可能となり、コンテンツ送信側機器からコンテンツ受信側機器にコンテンツを送信する際、コンテンツ送信側機器から所望のコンテンツ受信側機器にコンテンツを盗取されずに確実に送信可能となる。

【図面の簡単な説明】

【図1】

本発明に係る第1のプロセスの一実施形態におけるソースデバイスの動作を示すフローチャートである。

【図2】

本発明に係る第1のプロセスの一実施形態におけるシンクデバイスの動作を示すフローチャートである。

【図3】

本発明に係る第2のプロセスの一実施形態におけるソースデバイスの動作を示すフローチャートである。

【図4】

本発明に係る第2のプロセスの一実施形態におけるシンクデバイスの動作を示すフローチャートである。

【図5】

鍵交換プロセスにおけるソースデバイスの動作を示すフローチャートである。

【図6】

鍵交換プロセスにおけるシンクデバイスの動作を示すフローチャートである。

【図 7】

コンテンツの伝送の際に考えられる不正なシンクデバイスを排除する過程を示す模式図である。

【図 8】

ソースデバイス及びシンクデバイスが有している格納手段に格納されている情報を示す模式図である。

【図 9】

本発明に係るソースデバイス及びシンクデバイスを構成する手段を示す模式図である。

【図 1 0】

ソースデバイスとシンクデバイスの様々な接続形態を示す図である。

【図 1 1】

本発明に係るソースデバイス（コンテンツ送信側機器）からシンクデバイス（コンテンツ受信側機器）にコンテンツを送信するために行われる手順の一実施形態を示すフローチャートである。

【図 1 2】

（a）は、情報 B の構成を示す模式図である。

（b）は、B org 証明情報を示す模式図である。

【図 1 3】

第 1 のプロセス、第 2 のプロセス、鍵交換プロセスにおけるソースデバイス及びシンクデバイスの動作をまとめて示すタイムチャートである。

【符号の説明】

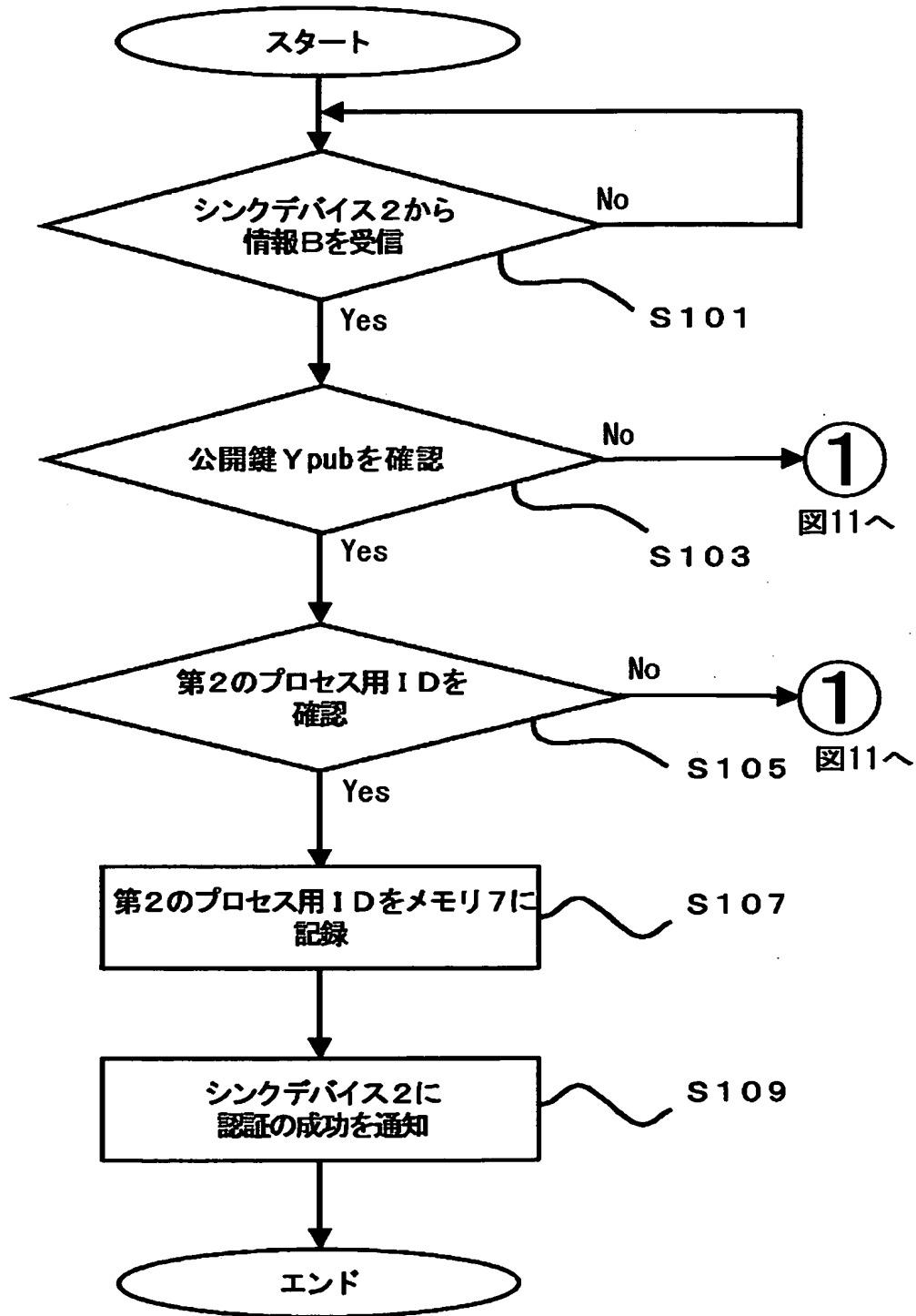
- 1 ソースデバイス（コンテンツ送信側機器）
- 2 シンクデバイス（コンテンツ受信側機器）
- 3 送信手段
- 4 受信手段
- 5 演算手段
- 6 格納手段
- 7 メモリ

8 照合手段

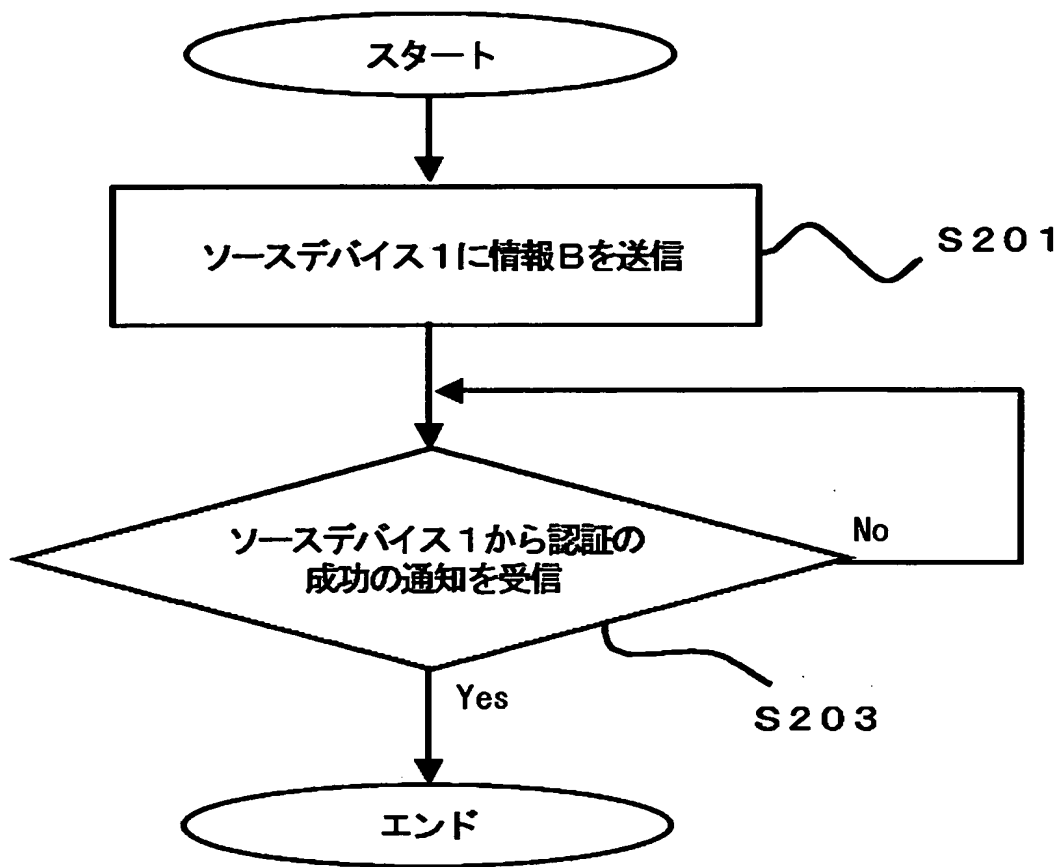
【書類名】

図面

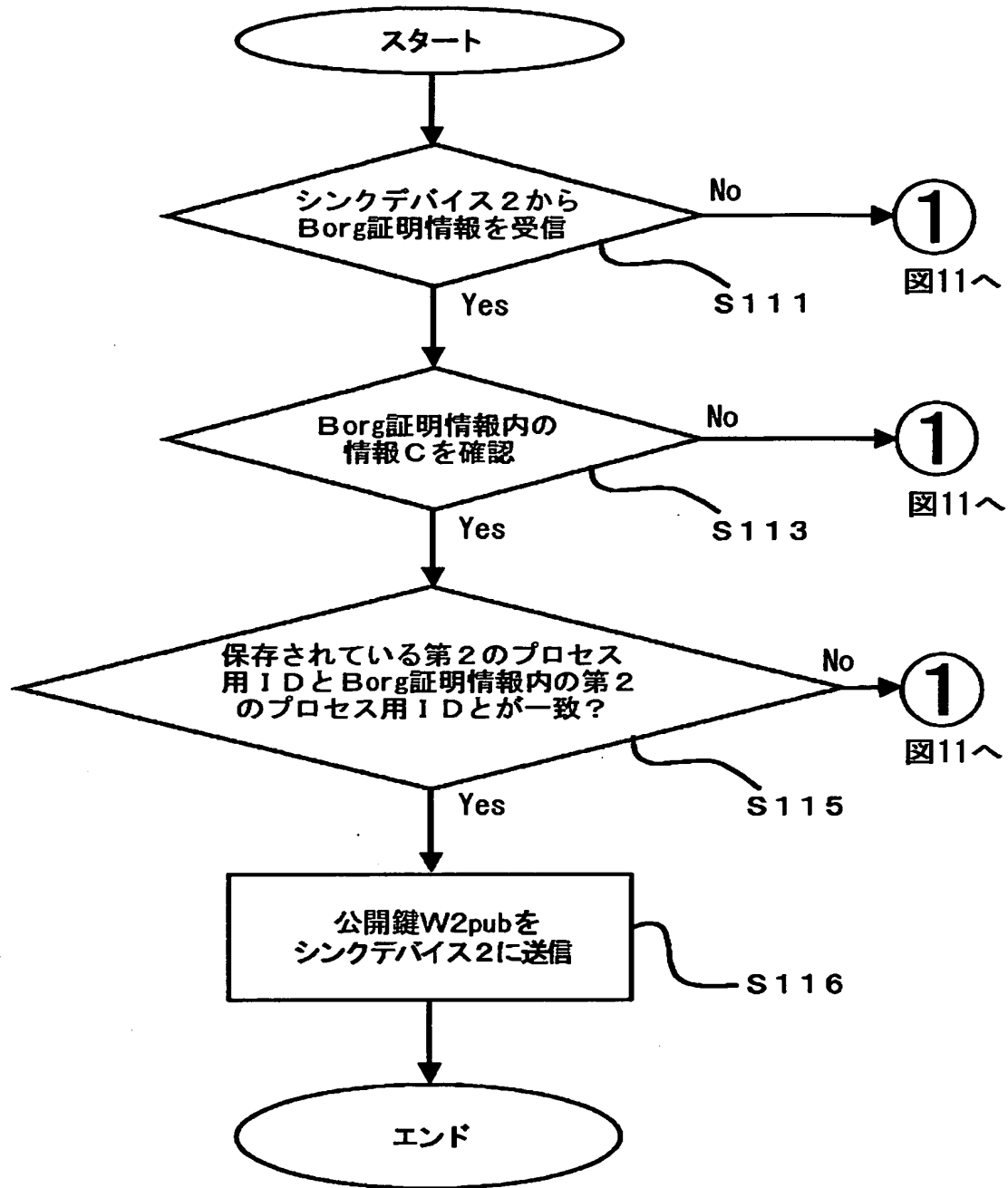
【図 1】



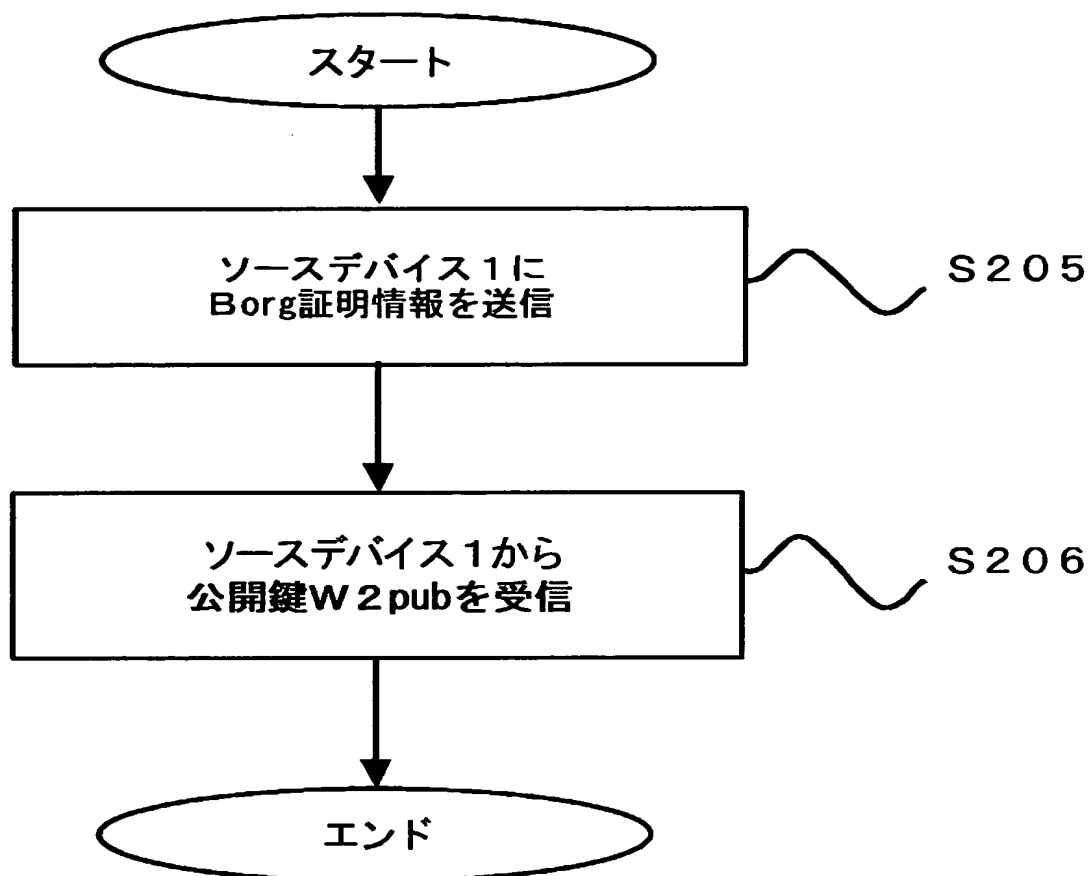
【図2】



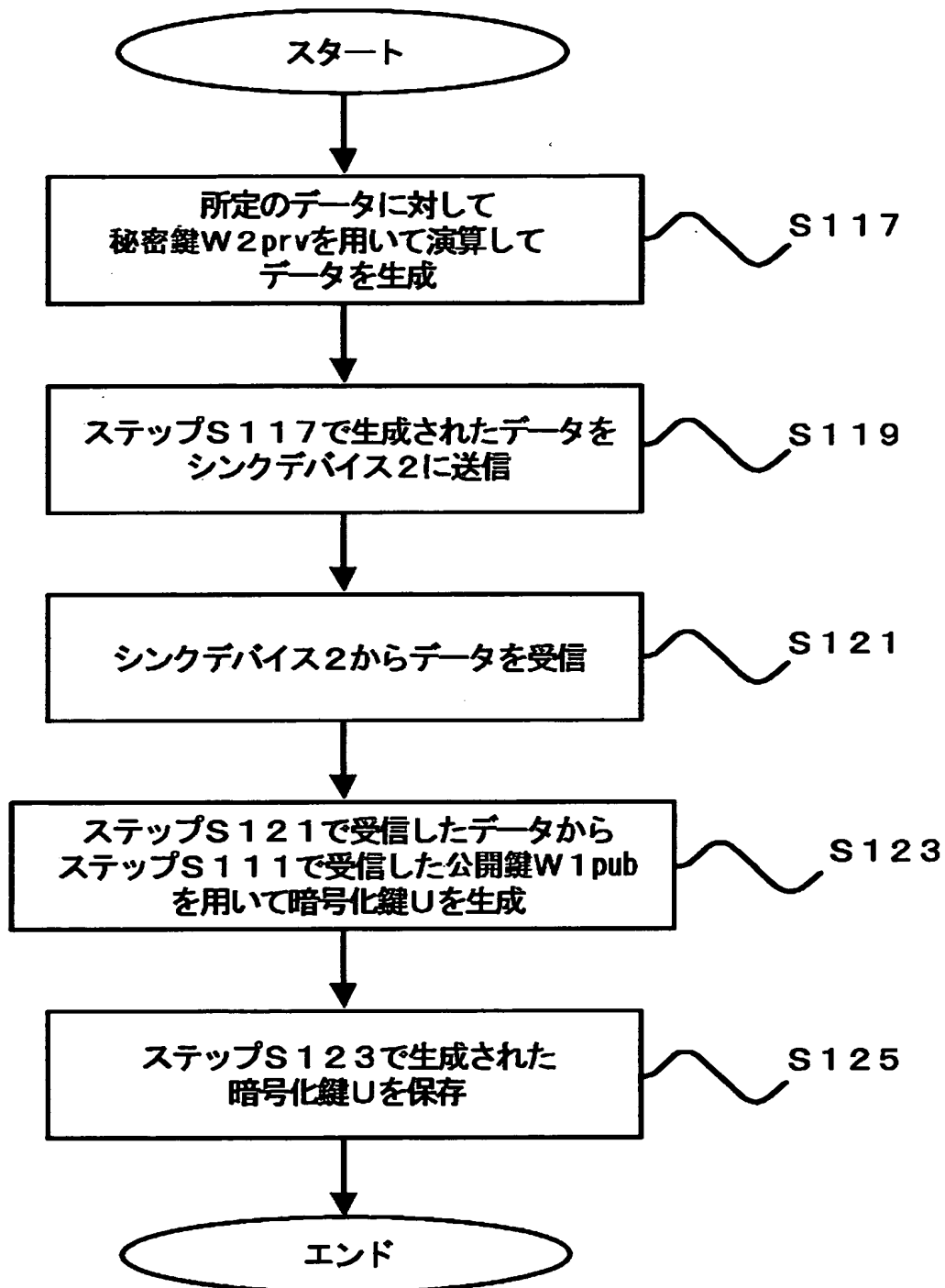
【図 3】



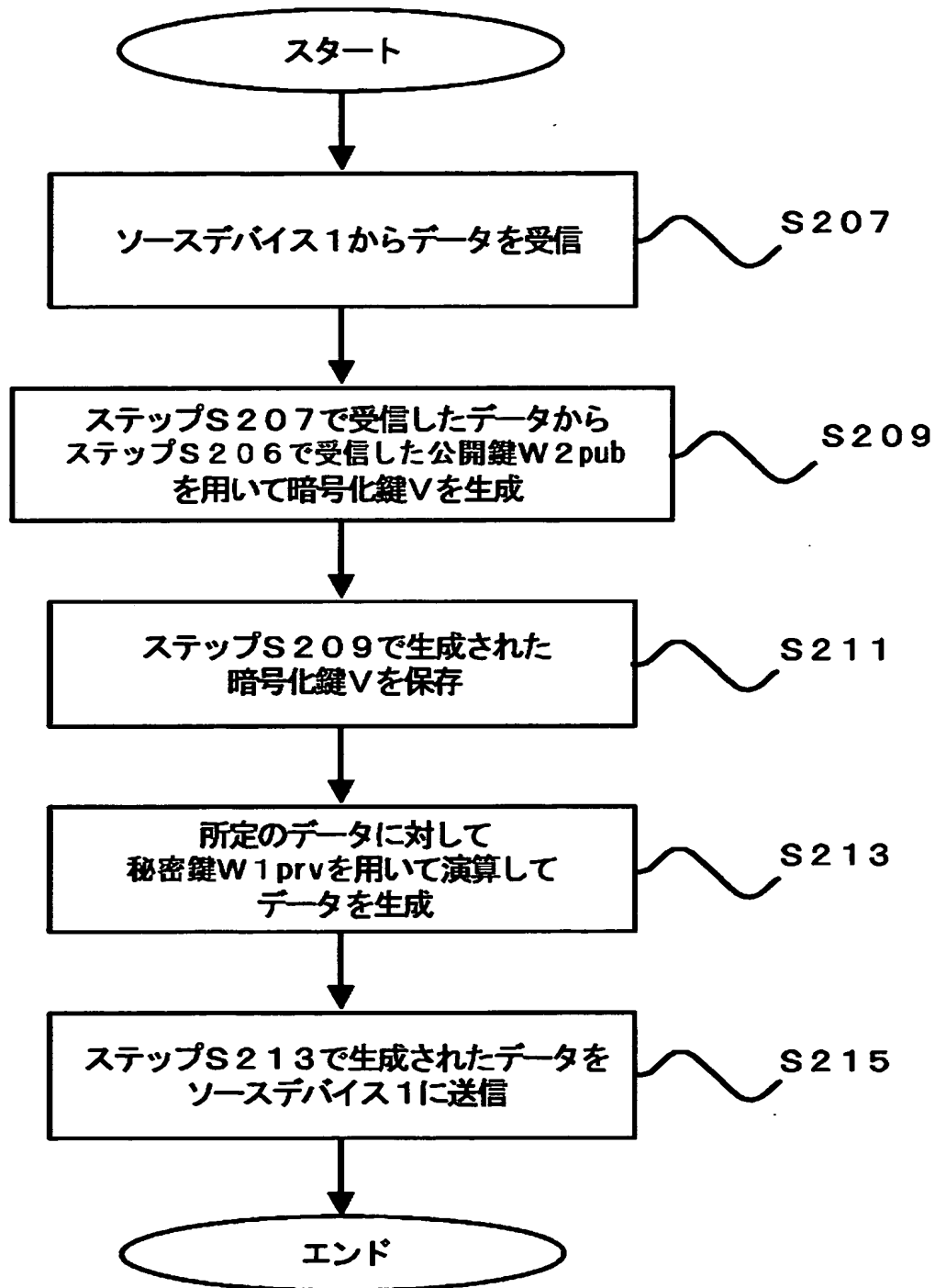
【図4】



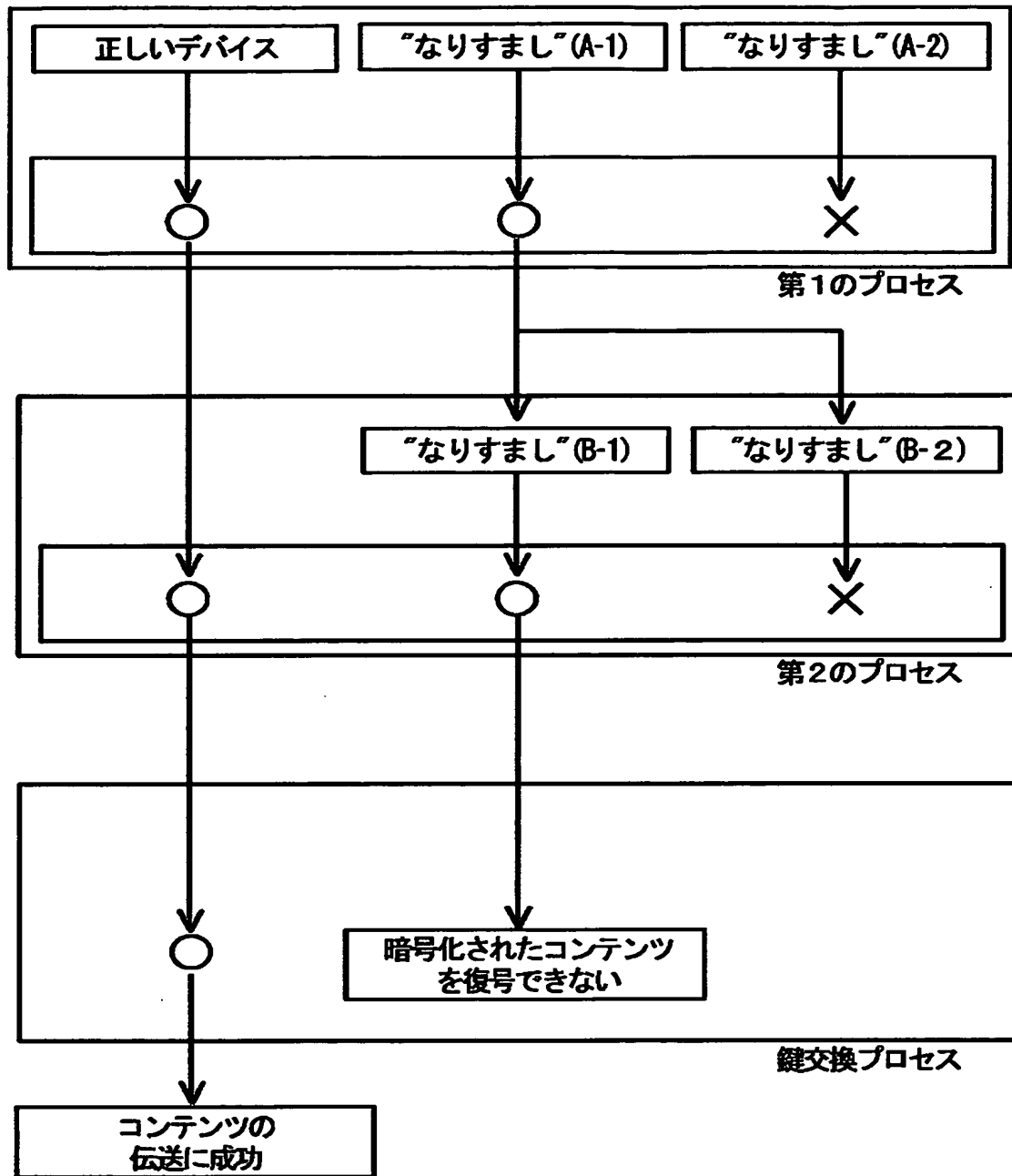
【図5】



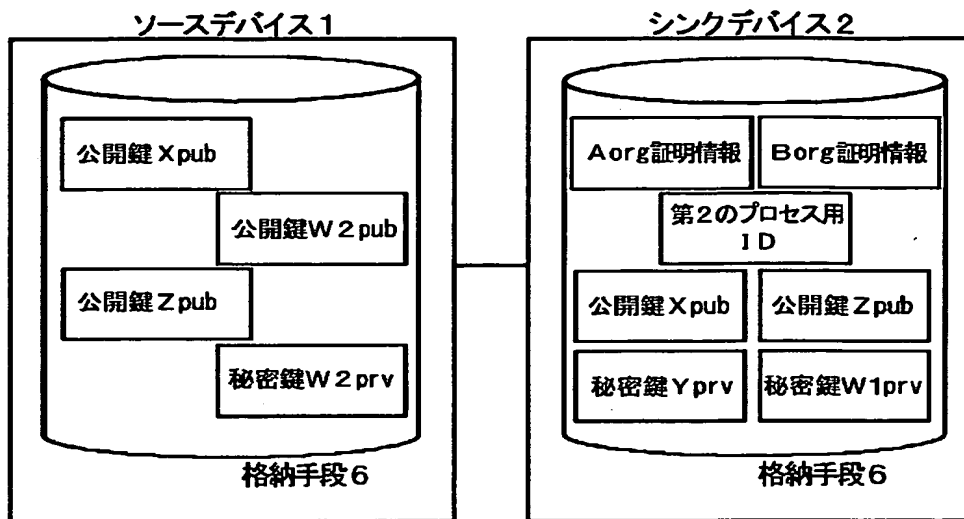
【図6】



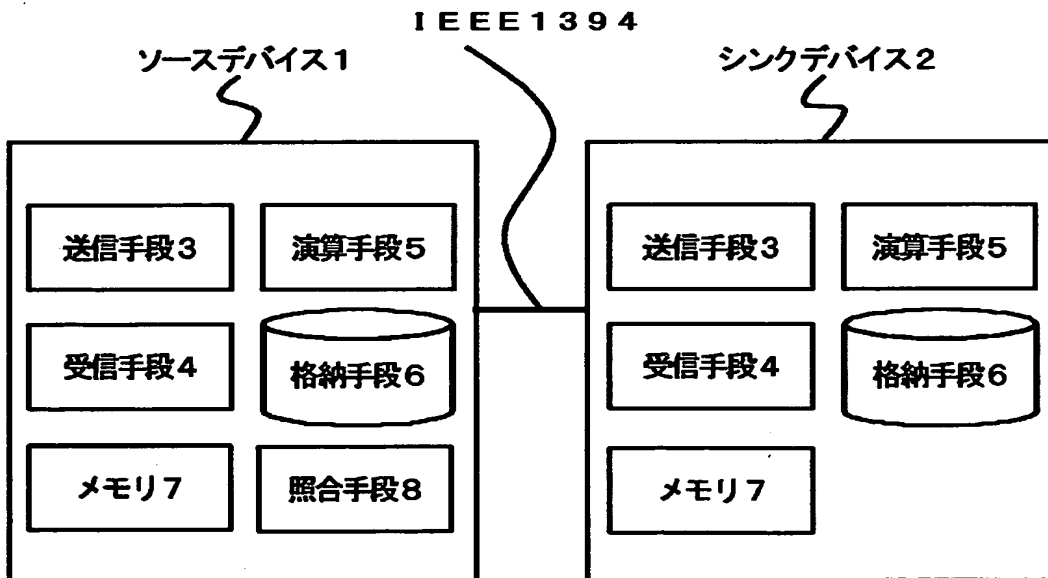
【図 7】



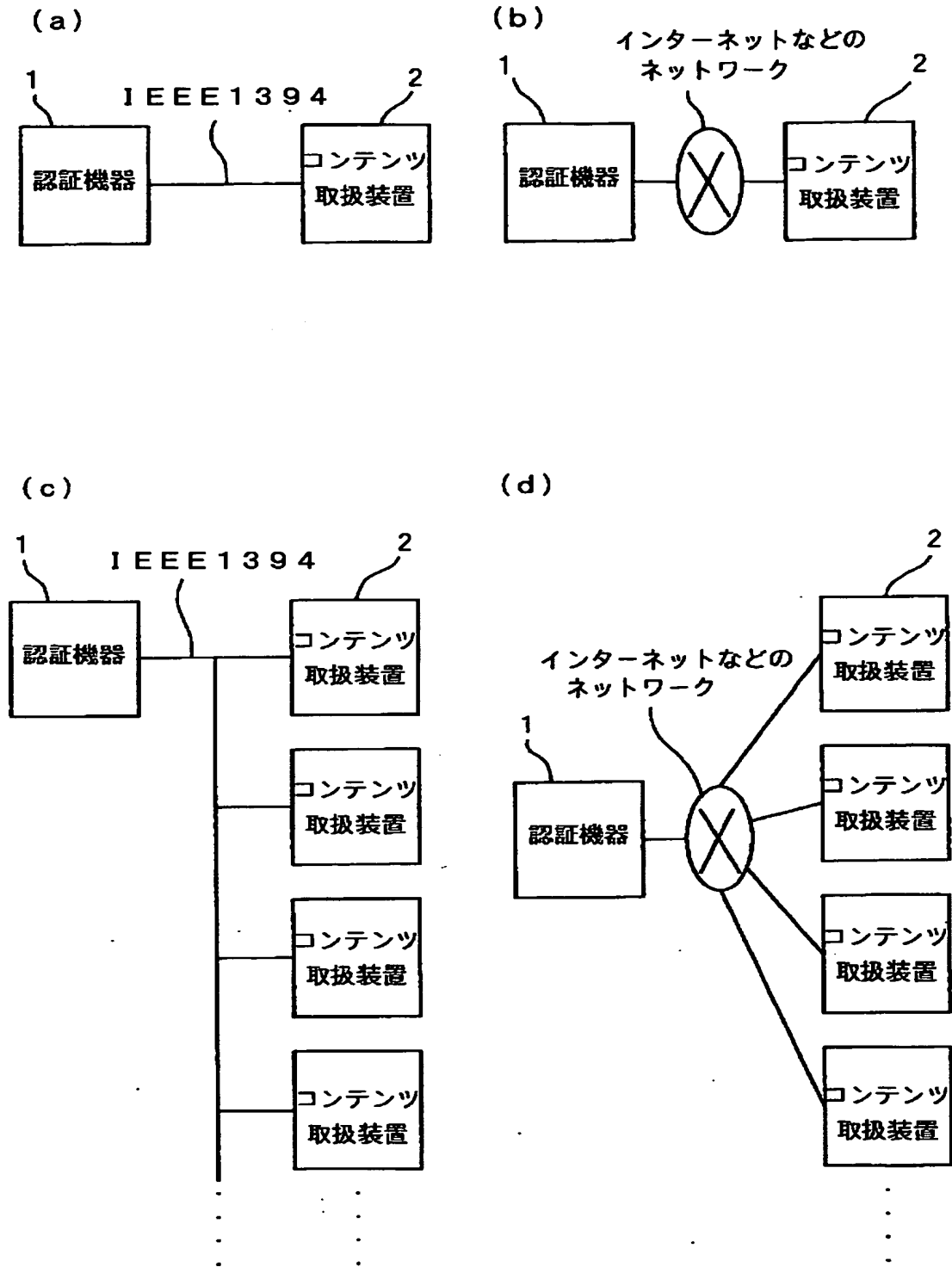
【図 8】



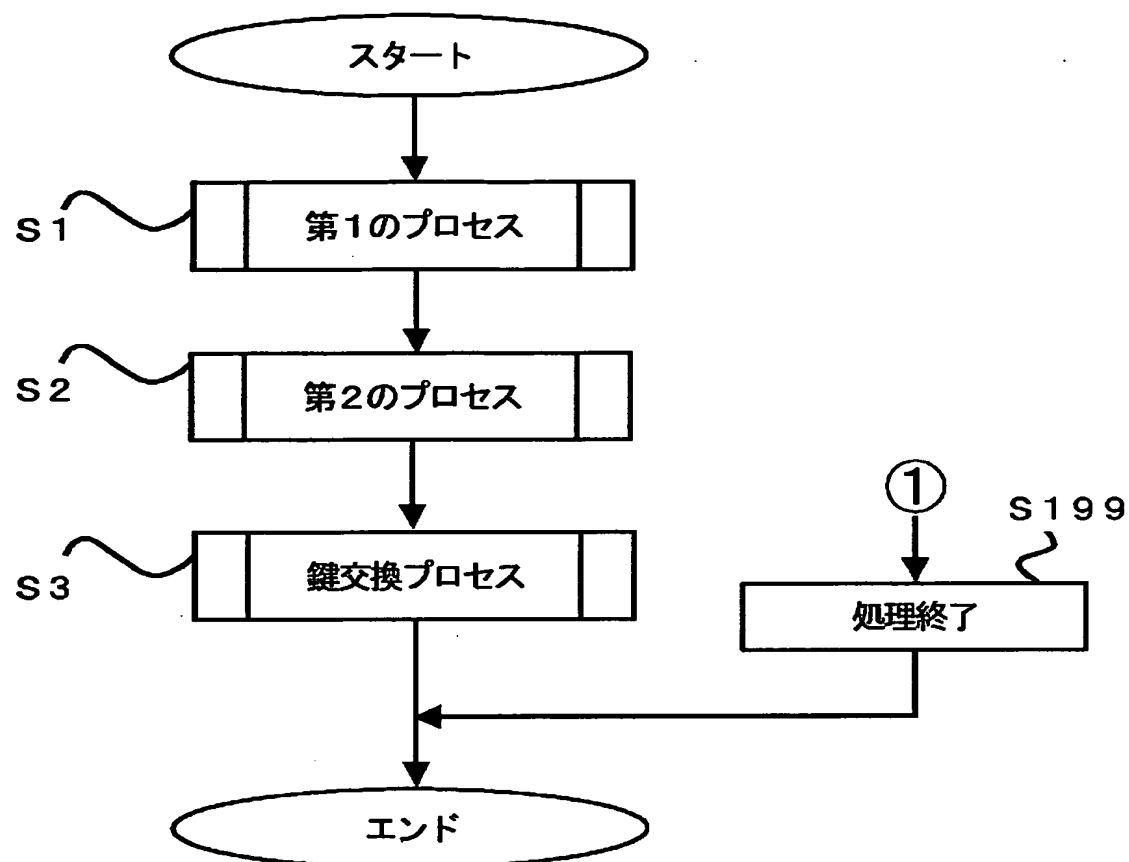
【図 9】



【図 1 0】

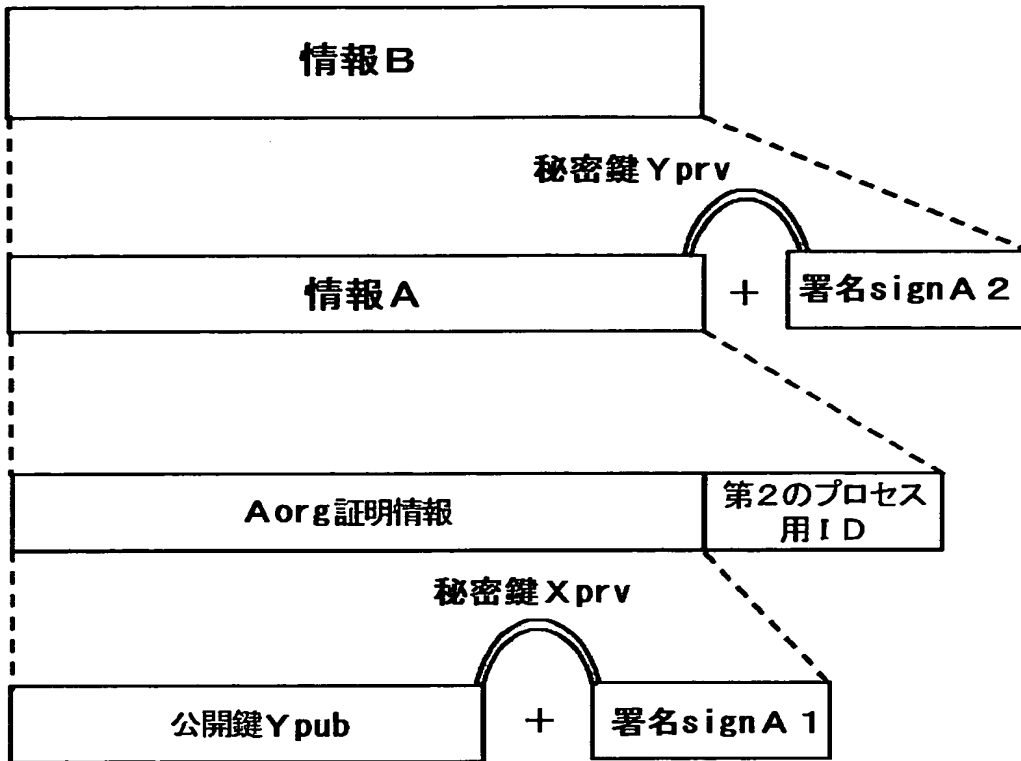


【図 1 1】

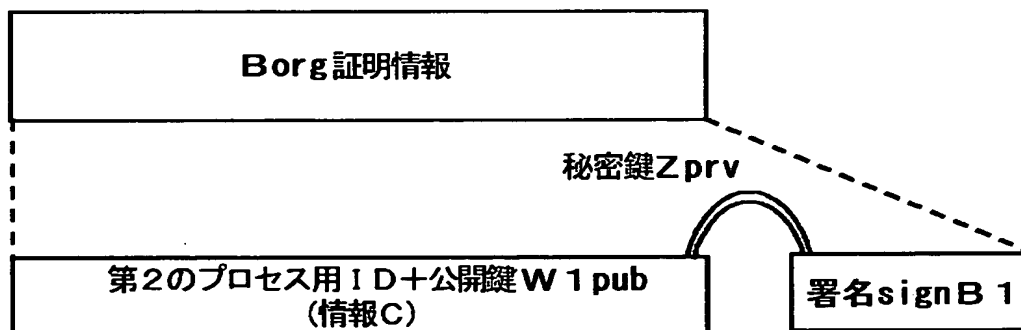


【図 1 2】

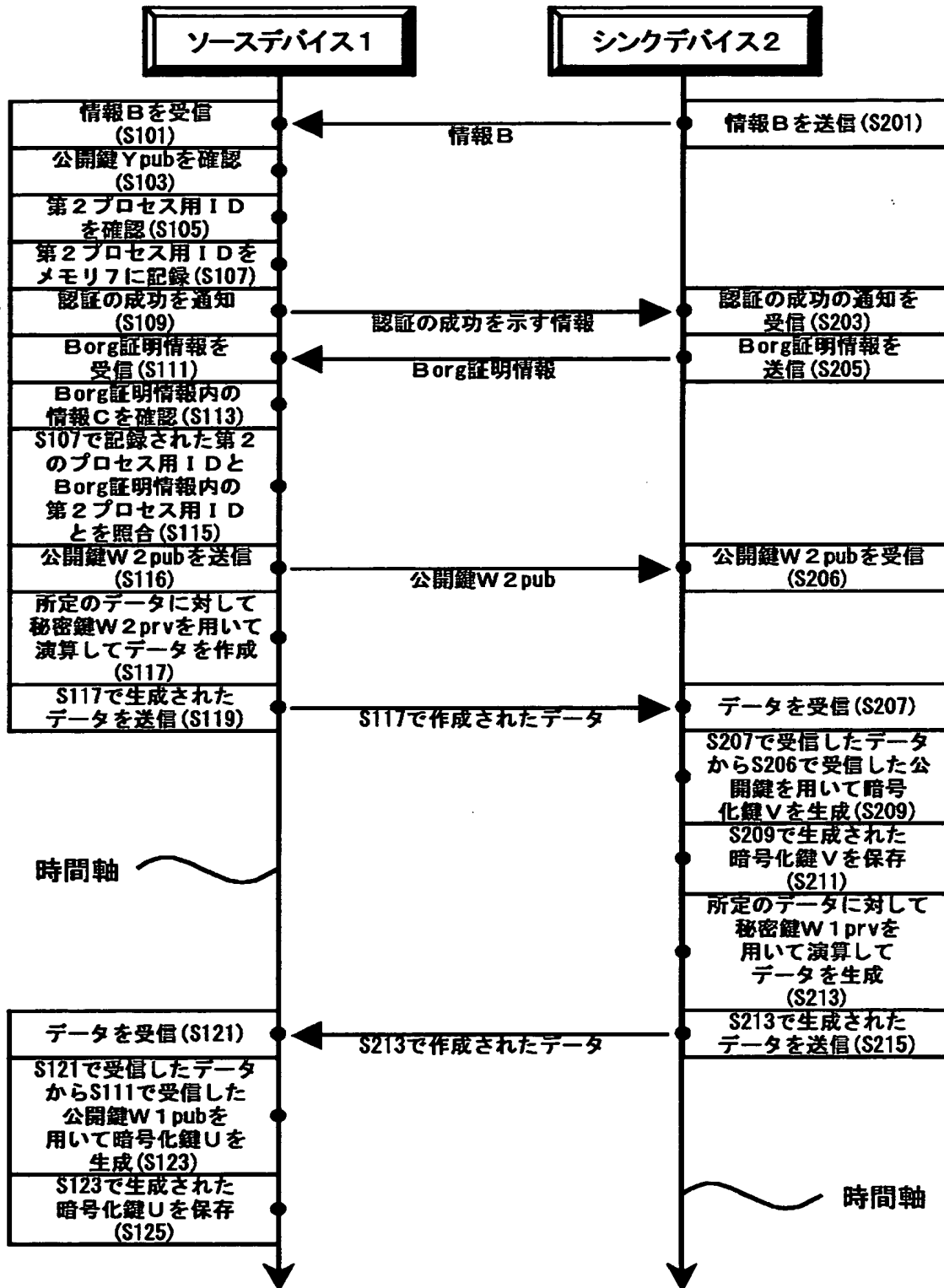
(a)



(b)



【図 13】



【書類名】 要約書

【要約】

【課題】 ソースデバイス（コンテンツ送信側機器）からシンクデバイス（コンテンツ受信側機器）にコンテンツを送信する際、コンテンツを盗取されずに所望のシンクデバイスに確実に送信可能となるよう認証を行う。

【解決手段】 第 1 の管理機関からライセンスを受けている証明となるシンクデバイス 2 の証明情報と第 2 の管理機関により管理されているシンクデバイス 2 の識別情報とが結合されたものに署名が付加された情報をシンクデバイス 2 からソースデバイス 1 に送信し、ソースデバイス 1 でその証明情報を認証し、さらにその証明情報を参照して署名を認証して、シンクデバイス 2 の識別情報を記録手段に記録する。続いて、再びシンクデバイス 2 の識別情報をシンクデバイス 2 からソースデバイス 1 に送信し、この情報を受信したソースデバイス 1 で、この情報と記録手段に記録されたシンクデバイス 2 の識別情報とを照合する。

【選択図】 図 9

認定・付加情報

特許出願の番号	特願2000-133957
受付番号	50000560557
書類名	特許願
担当官	第七担当上席 0096
作成日	平成12年 5月 8日

<認定情報・付加情報>

【提出日】	平成12年 5月 2日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000004329]

1. 変更年月日 1990年 8月 8日
[変更理由] 新規登録
住 所 神奈川県横浜市神奈川区守屋町3丁目12番地
氏 名 日本ビクター株式会社